802.1X认证的配置在WAP121和WAP321接入点的

客观

在802.1X认证，当主机(亦称请求方)时设法连接到安全网络，网络设备呼叫证明人检查用支持安全协议， RADIUS和可扩展的认证协议(EAP)的认证服务器，验证请求方的身份。这样，网络设备提供安全一个另外的层给网络。

本文解释如何配置WAP121和WAP321接入点作为802.1X认证的一请求方。

可适用的设备

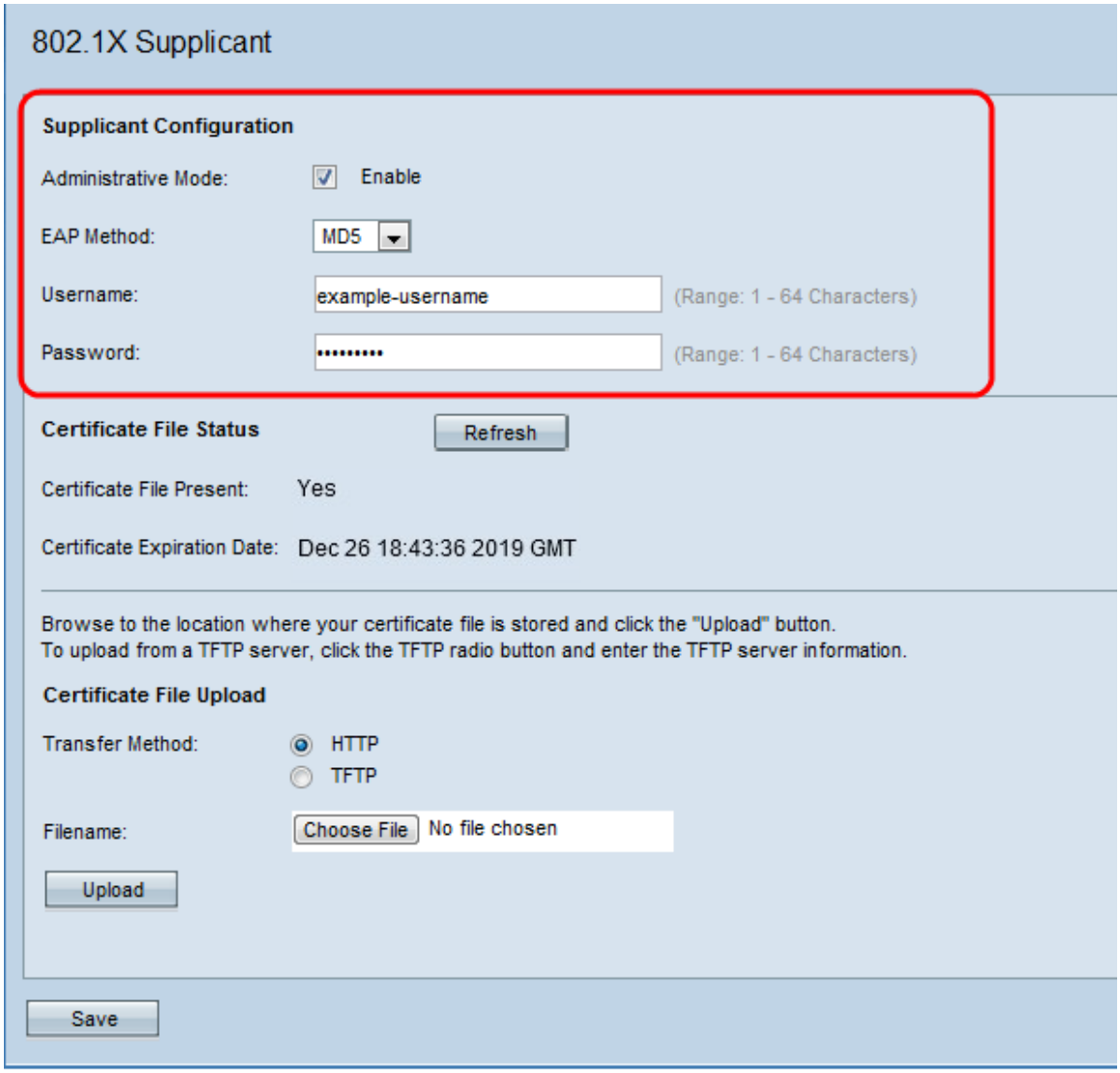
- WAP121
- WAP321

软件版本

- 1.0.3.4

802.1X请求方配置

步骤1.登陆到Web配置工具并且选择**系统安全> 802.1X请求方**。*请求方*配置页打开：



Step 2.检查在管理模式字段的**Enable (event)**对enable (event)设备作为在802.1X认证的一请求方。

步骤3.从在EAP方法字段的下拉列表选择可扩展的认证协议(EAP)方法正确的类型。

- MD5 — MD5是用于加密所有大小数据到128位的算法，加密数据的MD5算法用途公共密钥加密系统。
- PEAP —保护的EAP是提供高级安全的认证方法，PEAP通过服务器发行的数字证书验证无线局域网客户端通过创建在客户端和认证服务器之间的一条被加密的SSL/TLS隧道。
- TLS —传输层安全(TLS)是为在互联网的通信提供安全和数据完整性的一个加密协议。当服务器和客户端沟通时，TLS保证第三方不窜改原始消息。大多MD5的功能用于TLS。

步骤4.输入接入点使用从在用户名和密码字段的802.1X证明人获得认证的用户名和密码。用户名和密码的长度必须是从1个到64个字母数字和符号字符。

步骤5.点击**"Save"**保存设置。

Note:证书文件状态地区显示是否证书文件存在。SSL认证是一个数字式地签名的证书由允许Web浏览器有安全通信用Web服务器的认证机关。要管理和配置SSL认证请参见*在WAP121和WAP321接入点的*条款*安全套接字层SSL证书管理*。